ПЕРЕЛІК ПИТАНЬ НА ЗАЛІК

1. Предмет та основні поняття дисципліни.
2. Конфіденційність, цілісність, доступність інформації.
3. Причини зростання комп’ютерної злочинності.
4. Значення інформаційної безпеки в житті суспільства.
5. Правозастосовча практика, діяльності правоохоронних органів по розкриттю і розслідуванню злочинів в сфері комп’ютерної інформації.
6. Визначення основ державної політики у сфері захисту інформації в автоматизованих системах.
7. Поняття і сутність комп'ютерної інформації, її відмінність від інших видів інформації.
8. Основні способи збереження комп'ютерної інформації.
9. Основні засоби передачі комп'ютерної інформації.
10. Основні засоби і методи захисту комп'ютерної інформації.
11. Об’єкт ідентифікації и встановлення дійсності.
12. Ідентифікація и встановлення дійсності особи.
13. Ідентифікація и встановлення дійсності технічних засобів.
14. Поняття атаки на комп’ютерну систему .
15. Атаки за допомогою соціальної інженерії.
16. Віддалені атаки через Internet.
17. Атаки з використанням CGI-додатків і Java аплетів.
18. Атаки типа Nuke. Атаки типа UDP. Атаки типа ICMP.
19. Атаки типа Spam.
20. Атаки на DNS.
21. Система Firewall з маршрутизатором і шлюзом.
22. Система Firewall на основі фільтрації пакетів.
23. Система Firewall на основі екранованого шлюзу.
24. Система Firewall на основі розміщення модемного пула.

25. Організація віртуальної корпоративної мережі (Virtual Private Network).

26. Методика розкриття і розслідування комп’ютерних злочинів.

27. Пошук і вилучення інформації и слідів впливу у ЕОМ и її пристроях.

28. Пошук і вилучення інформації и слідів впливу поза межами ЕОМ.

29. Використання спеціальних знань і призначення експертиз.

30. Обставини, що сприяють комп'ютерним злочинам.

31. Попередження комп'ютерних злочинів.

32. Галузі використання мережених програмно–апаратних систем безпеки, які призначені для автоматизованого забезпечення спостереженності комп'ютерних (обчислювальних) систем користувачів автоматизованої системи.